Mathematics 312, Summer 2019
Practice problems for the final exam

Problem 1. Suppose $a, b, c, d, n$ are positive integers, $a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$, $c$ is divisible by $a$ and $d$ is divisible by $b$. Can we conclude that $c/a \equiv d/b \pmod{n}$? If so, give a proof. If not, give a counterexample.

Problem 2. Let $n$ be an integer. Show that there does not exist a prime number $p \geq 2$ which divides both $8n + 3$ and $5n + 2$.

Problem 3. Let $n = 3^{100}$ and $a = 8585 \ldots 85$ be the $2n$-digit number, where the digits 85 repeat $n$ times.
(a) Is $a$ divisible by 9?
(b) Is $a$ divisible by 11?
Explain your answers.

Problem 4. Find all three-digit combinations that can occur as the last three digits of $a^{100}$, where $a$ ranges over the integers. Give a simple criterion for predicting which of these possibilities occurs for a given $a$, without computing $a^{100}$. Prove that your criterion is correct.

Hint: Investigate $a^{100}$ modulo 8 and modulo 125 separately, then use the Chinese Remainder Theorem.

Problem 5. Suppose a positive integer $n$ has 77 positive divisors (1 and $n$ count among them). How many of these divisors can be primes? Explain your answer.

Problem 6. Find all positive integers $n$ such that $\phi(n) = 22$ and prove that there are no others. Here $\phi$ denotes the Euler $\phi$-function.

Problem 7. Recall that an affine cryptosystem, with encryption key $K_E = (26, a, b)$ and decryption key $K_D = (26, c, d)$ works as follows. Each letter is assigned a numerical value, in alphabetical order: $A \mapsto 0$, $B \mapsto 1$, ..., $Z \mapsto 25$. These numbers are then viewed modulo 26: they are encrypted by the formula
\[ x \rightarrow y \equiv ax + b \pmod{26} \]
and decrypted by the formula
\[ y \rightarrow x \equiv cy + d \pmod{26}. \]
It is known that the most frequently occurring letter in the English language is $E$ (with numerical value 4) and the second most frequently occurring letter is $T$ (with numerical value 19). Suppose these letters are encoded as $F$ (numerical value 5) and $G$ (numerical value 6), respectively.

(a) Find the encryption key $K_E$.
(b) Find the decryption key $K_D$.

Problem 8. Suppose the public key for an RSA cryptosystem is $(n, e) = (85, 7)$ and the secret key is $(85, d)$. Show that this cryptosystem is not secure by finding $d$.

Remarks: Recall that a message $x$ is encoded by $x \rightarrow x^e \pmod{n}$ and a received message $y$ is decoded by $y \rightarrow y^d \pmod{n}$. To make this cryptosystem secure, one needs to use a much larger $n$. 